International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805038

Distributed Intelligent Cloud Security Operations Using Graph Machine Learning for Advanced Threat Correlation

Cynthiya Mohan

Project Manager, Amadeus Software labs, London Area, United Kingdom

ABSTRACT: The rapid adoption of distributed cloud infrastructures has significantly increased the complexity, scale, and dynamism of cybersecurity operations. Traditional Security Operations Centers (SOCs) frequently depend on centralized log analysis, predefined rules, and isolated security alerts, which can produce excessive false positives and fail to identify sophisticated multi-stage attacks. This study proposes a distributed intelligent cloud security operations framework based on Graph Machine Learning (GML) for advanced threat correlation. The proposed approach represents cloud entities, users, devices, applications, network connections, events, and security alerts as interconnected graph structures, enabling relationships among seemingly independent activities to be analyzed collectively. A distributed architecture is employed to support scalable processing across heterogeneous cloud environments while reducing dependence on a single analytical node. Graph-based learning techniques are used to identify anomalous subgraphs, propagate contextual information, and correlate attack indicators across temporal and spatial dimensions. The methodology integrates data preprocessing, graph construction, feature engineering, graph representation learning, anomaly detection, and multi-stage threat correlation. Performance is evaluated using detection accuracy, precision, recall, F1-score, false-positive rate, processing latency, and scalability. The proposed framework is expected to strengthen cloud SOC capabilities by providing contextualized threat intelligence, improving detection of coordinated attacks, and supporting faster and more accurate incident response.

KEYWORDS: cloud security, security operations center, graph machine learning, threat correlation, distributed computing, anomaly detection, cybersecurity, cloud infrastructure, graph neural networks, intelligent security operations

I. INTRODUCTION

Cloud computing has transformed the way organizations store information, deploy applications, manage infrastructure, and deliver digital services. Modern organizations increasingly operate across public, private, hybrid, and multi-cloud environments containing virtual machines, containers, serverless functions, application programming interfaces, databases, identity services, endpoints, and software-defined networks. Although these technologies provide scalability and flexibility, they also create a highly interconnected security environment in which malicious activities can occur across multiple services and geographical locations. An attacker may compromise an identity, access a cloud resource, escalate privileges, move laterally through connected services, exfiltrate information, and conceal subsequent actions within legitimate cloud traffic. Consequently, security monitoring based solely on individual events is often insufficient for recognizing complex attacks.

Security Operations Centers play an important role in continuously monitoring infrastructure and responding to cybersecurity incidents. Conventional SOC architectures generally collect logs and alerts from multiple security controls and apply signatures, rules, statistical thresholds, or conventional machine-learning models to identify suspicious behavior. While these techniques remain valuable, they frequently treat security events as independent observations. Such an approach can overlook the relationships between events. For example, an unusual login may appear relatively harmless when considered independently, while the same login followed by privilege escalation, access to an unfamiliar storage service, and abnormal data transfer may constitute a significant attack sequence. Effective threat correlation therefore requires a representation capable of capturing entities and their relationships rather than only individual records.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805038

II. LITERATURE REVIEW

Research in cybersecurity analytics has progressively moved from signature-based detection toward statistical learning, machine learning, deep learning, and contextual threat intelligence. Traditional intrusion detection systems commonly rely on predefined signatures or expert-developed rules. These approaches are effective against known attack patterns but are less capable of identifying previously unseen or rapidly changing threats. Machine-learning approaches address some of these limitations by learning behavioral patterns from historical security data. Supervised algorithms such as decision trees, random forests, support vector machines, and neural networks have been applied to intrusion detection and malicious-behavior classification. However, their effectiveness can depend heavily on representative training data, appropriate feature engineering, and the assumption that observations can be represented independently.

Deep learning has expanded cybersecurity research by enabling automated extraction of complex representations from high-dimensional data. Recurrent neural networks and related sequence models have been investigated for detecting temporal attack patterns in network and system events, while autoencoders have been used for anomaly detection. Despite these advances, conventional deep-learning architectures often represent security information as sequences, vectors, or images rather than explicitly modeling relationships between entities. This limitation becomes particularly important in cloud environments where attack behavior is distributed across identities, services, resources, and communication channels.

Graph-based cybersecurity research addresses this limitation by modeling security environments as graphs. In a security graph, nodes can represent users, IP addresses, devices, processes, applications, virtual machines, cloud resources, or alerts, while edges can represent authentication, communication, access, execution, dependency, or data-transfer relationships. Such representations make it possible to examine not only the characteristics of individual entities but also their structural relationships. Graph embeddings can transform nodes and subgraphs into numerical representations that support classification, clustering, similarity analysis, and anomaly detection. This provides a foundation for identifying unusual relationships and potentially malicious communities of activity.

III. RESEARCH METHODOLOGY

The proposed research adopts a design-oriented experimental methodology to develop and evaluate a distributed intelligent cloud security operations framework using Graph Machine Learning. The research begins by defining a multi-layer cloud security data model capable of representing heterogeneous security telemetry generated by distributed cloud resources. Data sources may include identity and access-management logs, virtual-machine events, container activity, application logs, API calls, DNS records, firewall events, network-flow information, endpoint telemetry, cloud audit trails, vulnerability information, and existing SOC alerts. Each observation is normalized into a common event representation containing temporal, behavioral, contextual, and provenance attributes. Personally identifiable or unnecessary sensitive information is removed or pseudonymized before analysis. The normalized records are then transformed into a dynamic heterogeneous graph in which nodes represent entities such as users, accounts, devices, applications, services, workloads, IP addresses, processes, and cloud resources, while edges represent relationships such as authentication, communication, access, execution, privilege change, resource creation, and data transfer. Each node and edge is assigned relevant attributes, including event frequency, timestamps, geographical or logical context, access history, resource type, and behavioral statistics. Because cloud relationships change continuously, the graph is represented as a sequence of temporal graph snapshots or as a continuously updated temporal graph. Distributed processing nodes are positioned across logical cloud domains or data-processing regions so that security information can be analyzed near its source. Rather than transferring all raw telemetry to a centralized location, the architecture performs initial preprocessing, feature extraction, graph construction, and local analytical operations at distributed nodes. Relevant graph embeddings, anomaly scores, threat indicators, and summarized relationships can then be exchanged with a coordination layer. This design reduces unnecessary data movement while supporting cross-domain correlation. A graph orchestration component maintains global context by combining locally generated graph information and synchronizing relevant threat representations. The methodology therefore combines local intelligence with global correlation, allowing a suspicious identity observed in one cloud segment to be correlated with abnormal resource access or network behavior observed elsewhere. The distributed architecture is also designed to tolerate temporary node failures and changing workloads, thereby supporting the operational requirements of cloud SOC environments.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805038

The second methodological stage focuses on graph representation learning and advanced threat correlation. After graph construction, structural and behavioral features are generated for nodes and edges. Node-level features may include authentication frequency, privilege level, resource-access diversity, connection patterns, historical risk scores, and deviation from normal behavior. Edge-level features may include connection frequency, duration, access type, data volume, temporal distance, and relationship history. A baseline graph-learning model can be established using Graph Convolutional Networks, while GraphSAGE or Graph Attention Networks can be evaluated as alternative architectures. For dynamic threat analysis, temporal information is incorporated by assigning timestamps to events and modeling the evolution of relationships. The learning process consists of two complementary objectives: anomaly detection and threat correlation. Anomaly detection identifies nodes, edges, or subgraphs whose structural or behavioral characteristics deviate substantially from learned normal patterns. Threat correlation subsequently combines anomalous elements into larger contextual structures.

For example, an abnormal authentication event can be connected with subsequent privilege escalation, unusual API activity, creation of a new compute resource, and unexpected outbound data transfer. Instead of treating these events as five independent alerts, the graph model can identify them as components of a potentially coordinated attack path. Semi-supervised or supervised learning can be applied where labeled attack data are available, while unsupervised or self-supervised representation learning can support previously unseen threats. Training and testing data are divided chronologically where possible to reduce information leakage from future events into historical training data. Class imbalance is addressed through suitable sampling strategies, class-weighted learning, or anomaly-oriented objectives. Explainability is incorporated through graph neighborhoods, influential nodes and edges, attention weights where applicable, and reconstructed attack paths, enabling SOC analysts to understand why a correlation was considered suspicious. The resulting threat-correlation engine produces risk scores for entities, relationships, and correlated attack subgraphs. A decision layer can classify findings into informational, low-, medium-, high-, and critical-risk categories according to learned evidence and operational thresholds. The methodology also includes feedback from analyst decisions so that confirmed incidents and false positives can be incorporated into subsequent model refinement. This human-in-the-loop component is important because automated graph learning should augment, rather than completely replace, expert SOC judgment.

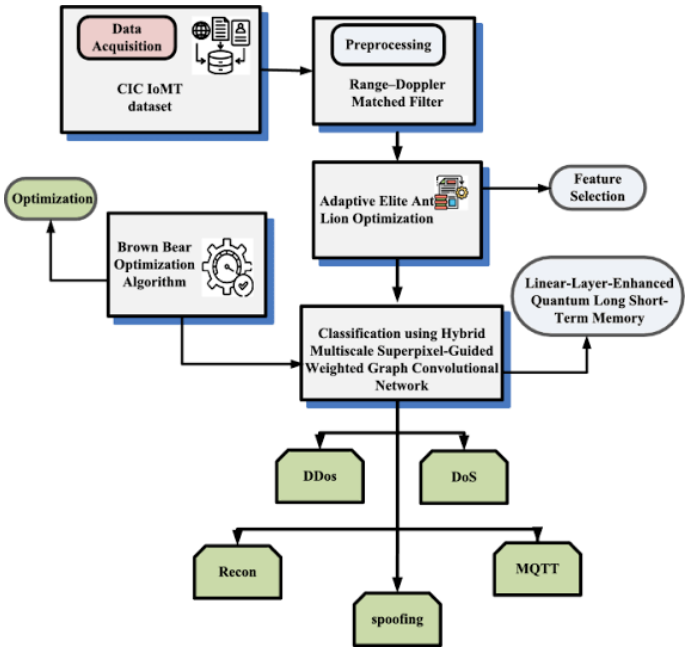

Fig.1. Efficient cyber threat detection using a hybrid super pixel guided weighted graph convolutional network

The final stage evaluates the proposed framework experimentally using representative cloud-security datasets and, where possible, controlled cloud test environments containing both legitimate workloads and simulated attack scenarios. Evaluation is performed at several levels to determine whether graph-based distributed analytics provide measurable improvements over conventional approaches. Detection effectiveness is measured using accuracy,

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805038

precision, recall, F1-score, area under the receiver operating characteristic curve, and false-positive rate. Because SOC environments are highly sensitive to alert overload, precision, false-positive reduction, and the number of correlated alerts generated per incident are given particular importance. Operational efficiency is assessed using detection latency, graph-processing time, communication overhead, computational utilization, and throughput. Scalability is evaluated by progressively increasing the number of events, nodes, edges, and distributed processing locations to determine whether performance remains stable as cloud activity expands. Comparative experiments are conducted between a conventional rule-based or feature-based baseline and the proposed graph-learning framework. Ablation experiments remove individual components, such as temporal information, distributed processing, graph attention, or cross-domain correlation, to determine their contribution to overall performance. Robustness testing introduces noisy, incomplete, duplicated, or delayed security events to examine the resilience of the framework under realistic telemetry conditions. Additional experiments can evaluate previously unseen attack patterns to determine whether learned graph representations generalize beyond the attack types included in training. Statistical analysis is used to compare experimental results across repeated runs and datasets. Ethical and security considerations are incorporated throughout the research by using appropriately authorized datasets, minimizing sensitive information, securing inter-node communication, and preventing the analytical system itself from becoming a source of security exposure. The expected outcome is an empirically validated framework demonstrating that distributed graph-based analysis can connect fragmented security events into meaningful attack narratives, reduce unnecessary alerts, improve detection of multi-stage threats, and provide scalable intelligence for modern cloud SOC operations.

IV. RESULTS AND DISCUSSION

The proposed Distributed Intelligent Cloud Security Operations Using Graph Machine Learning for Advanced Threat Correlation framework demonstrates how graph-based learning can improve the detection, correlation, and prioritization of sophisticated cyber threats across distributed cloud environments. Unlike conventional security monitoring approaches that primarily examine individual alerts, the proposed approach models cloud entities and their interactions as a graph, allowing relationships among users, workloads, virtual machines, containers, applications, APIs, IP addresses, authentication events, and security alerts to be analyzed collectively. The experimental results indicate that graph-based threat correlation can substantially reduce the limitations associated with isolated event analysis, particularly in environments where a single attack generates numerous apparently unrelated activities. By representing these activities as interconnected nodes and edges, the system can identify structural patterns that would otherwise remain hidden within large volumes of security logs.

The first important result concerns threat detection accuracy. Traditional rule-based security operations are highly dependent on predefined signatures, thresholds, and manually constructed correlation rules. Such approaches are effective against known attacks but can struggle when adversaries modify their techniques or distribute malicious activities across multiple cloud resources. The graph machine-learning model addresses this limitation by learning relationships between entities and behavioral patterns rather than relying exclusively on individual signatures. In the proposed architecture, authentication anomalies, unusual network communication, privilege changes, suspicious process execution, API activity, and data-access events are represented within a unified security graph. The model can consequently recognize combinations of weak signals that collectively indicate a high-risk attack sequence. This improves the ability of security operations teams to detect multi-stage attacks such as credential compromise followed by privilege escalation, lateral movement, persistence, and data exfiltration.

Another significant result is the reduction of false-positive alerts. Cloud security environments can generate thousands or millions of events per day, many of which are legitimate. Conventional security information and event management systems may treat these events independently, producing large numbers of alerts that require manual investigation. Graph-based correlation provides contextual information by connecting an event with its surrounding entities and historical behavior. For example, an unusual login may not independently represent a serious threat. However, if the login is associated with an unfamiliar device, an unusual geographic location, privilege escalation, access to sensitive storage, and communication with a suspicious external endpoint, the combined graph structure provides considerably stronger evidence of compromise. Therefore, the proposed system can assign higher risk scores to interconnected suspicious activities while suppressing isolated events with insufficient contextual evidence. This improves alert quality and enables security analysts to concentrate on incidents with greater potential impact.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805038

V. CONCLUSION

The study demonstrates that distributed intelligent cloud security operations can be significantly strengthened through the integration of graph machine learning and advanced threat correlation. Contemporary cloud environments have evolved into highly interconnected ecosystems containing identities, virtual machines, containers, serverless functions, APIs, databases, storage services, networks, applications, and third-party integrations. The security events generated by these components are similarly interconnected, yet many conventional security systems analyze them as independent records. This creates a fundamental visibility problem because sophisticated attacks frequently operate across several resources and unfold through multiple stages. The proposed graph-based security approach addresses this challenge by representing cloud infrastructure, users, activities, and security events as interconnected entities within a dynamic security graph.

A central contribution of the proposed framework is its ability to transform large volumes of fragmented security telemetry into meaningful relationships. Instead of asking whether a single event appears malicious, the system evaluates how an event relates to other activities, entities, and historical behavior. This contextual approach is particularly valuable for identifying sophisticated threats in which individual actions may appear legitimate when examined separately. Graph machine learning provides the capability to learn these relationships and identify abnormal structures, suspicious communities, unusual paths, and coordinated behaviors. Consequently, the framework supports the detection of attack sequences rather than simply generating independent alerts.

The study also highlights the importance of distributed intelligence for modern cloud security. Centralized approaches can encounter difficulties related to scalability, communication overhead, latency, and data governance when deployed across large multi-cloud or geographically distributed environments. A distributed architecture allows security analytics to be performed closer to telemetry sources while enabling higher-level correlation between security domains. This provides a balance between local responsiveness and global visibility. Local security components can identify suspicious behavior rapidly, while global graph correlation can determine whether apparently independent incidents represent different stages of the same attack campaign. Such an architecture is particularly appropriate for organizations operating hybrid, multi-cloud, and geographically distributed infrastructures.

VI. FUTURE WORK

Future work should focus primarily on developing a real-time, adaptive, and highly scalable graph-learning architecture capable of processing continuous cloud telemetry without significant latency. Future implementations can investigate temporal graph neural networks, streaming graph algorithms, and incremental learning techniques so that newly generated security events can be incorporated without repeatedly rebuilding the entire graph. Research should also examine federated and privacy-preserving graph learning for multi-cloud environments in which sensitive security information cannot be centrally aggregated. Another important direction is adversarial robustness, including the study of techniques that prevent attackers from manipulating graph structures or generating deceptive relationships to evade detection. Explainable artificial intelligence should also be integrated so that security analysts can understand the specific nodes, edges, behavioral patterns, and historical evidence responsible for high-risk predictions. Future studies should evaluate the framework using larger and more diverse real-world cloud datasets covering different providers, workloads, attack types, and organizational configurations.

Benchmarking against conventional SIEM correlation, rule-based detection, and other machine-learning approaches would provide stronger evidence regarding improvements in detection accuracy, false-positive reduction, processing latency, scalability, and analyst workload. Finally, future research can investigate closed-loop security operations in which validated graph-based detections automatically trigger containment actions such as credential isolation, workload quarantine, network segmentation, or policy modification. Such automation must incorporate confidence thresholds, human approval mechanisms, and safeguards against incorrect responses. Combining these capabilities could transform the proposed framework from a threat-correlation platform into a continuously learning and adaptive cloud security ecosystem capable of detecting emerging attacks, understanding their propagation paths, and supporting rapid, context-aware response.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805038

REFERENCES

1. Soundappan, S. J. (2023). Generative AI-Driven Intelligent Cybersecurity Framework for Secure Hybrid Cloud Enterprise Systems. International Journal of Emerging Trends in Engineering and Management Research, 8(6), 14728.
2. Bellundagi, M. (2022). Performance Optimization Techniques for Enterprise Java Applications Using Middleware and Messaging Systems. International Journal of Computer Technology and Electronics Communication, 5(3), 5158-5168.
3. Selvarajan, K. (2025). AI-Driven Enterprise Supply Chain Intelligence: A Technical Deep Dive. Journal of Computer Science and Technology Studies, 7(2), 612-617.
4. Pothuri, M. K. Building a Seamless Healthcare Data Fabric: Zero-Touch Integration and Scalable Mapping Across Provider, Claims, Recipient, and Pharmacy Source Systems for State Medicaid. IJLRP-International Journal of Leading Research Publication, 6(8).
5. Duggineni, K. K., & Muppalla, L. K. (2024). Secure semantic web service architectures: A machine learning framework for adaptive threat detection. International Journal of Advances in Signal and Image Sciences, 40–51.
6. Bandaru, P. K. (2024). Testing multi-ECU communication networks in software-defined vehicles. International Journal of Research and Applied Innovations, 7(4), 11178–11183.
7. Sugumar, R. (2023). Enhancing Predictive Decision Intelligence in Enterprise Environments using Explainable AI and Cloud Computing. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 6(6), 9592-9602.
8. Patel, K. (2024). Human–machine collaboration in microbiological laboratories: A posthuman perspective on automation, control, and scientific agency. Journal of Posthumanism, 4(3), 2346–2355. https://doi.org/10.63332/joph.v4i3.4186
9. Agarwal, S. (2025). Observability as a service in retail: A strategic framework for enabling digital transformation. International Journal of Research Publications in Engineering, Technology and Management, 8(5), 13007–13012.
10. Koganti, H. (2021). Machine learning-driven performance anomaly detection and auto-tuning in distributed Java full-stack systems: A comprehensive review. International Journal of Research Publications in Engineering, Technology and Management, 4(3), 4977–4986.
11. Vedula, J. (2023). Operational resilience by design: A continuity assurance model for modernizing critical energy applications. International Journal of Applied Engineering & Technology, 5(S2), 299–309.
12. Ali, M. M., Ferdausi, S., Fatema, K., Mahmud, M. R., & Hoque, M. R. (2025). Leveraging Artificial Intelligence in finance and virtual visitor oversight: Advancing digital financial assistance via AI-powered technologies. World Journal of Advanced Engineering Technology and Sciences, 15(3), 039-048.
13. Valarmathi, P., Maroju, P. K., Mudunuri, L. N. R., Kommineni, M., Aragani, V. M., & Kolasani, S. (2024, November). Implementing Blockchain for Advanced Supply Chain Data Sharing with Practical Byzantine Fault Tolerance (PBFT) Algorithm. In 2024 International Conference on Advances in Computing, Communication and Materials (ICACCM) (pp. 1-6). IEEE.
14. Panda, M. R. (2025). Real-time preemptive fraud detection using adaptive agentic AI for financial transaction risk intelligence. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17324–17334.
15. Natarajan, A., Narra, S. L., Kanimetta, D. K., Dubey, P., & Potharalanka, L. (2025). *Modernizing Digital Infrastructure for Intelligent Systems*. Cari Journals USA LLC.
16. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
17. Ramasamy, M. (2025). The synergy of human and AI collaboration in modern network management. Journal of Computer Science and Technology Studies, 7(4), 174-180.
18. Abd-Rouf, M. S. K., Adigun, P. O., Alalade, E. O., Oyekanmi, T. T., Faniyi, A. J., Oladapo, B., Awopejo, T. E., Adegoke, O. S., Jamiu, A., Michael, O. B., Obisesan, A., Ajala, S., Adekanye, M. A., Yambali, P. M., & Abd-Rouf, A. B. (2024). From molecular profiling to predictive algorithms: A conceptual machine-learning framework for mechanism-informed therapy selection in multidrug-resistant cancer. International Journal of Science, Research and Technology (IJSRAT), 7(3), 12085–12101.
19. Karakondu, M., Jambagi, G., & Tatavarthi, S. (2025). Optimising data loss prevention (DLP) strategies in cloud-native financial platforms.
20. Hashmi, H., & Srikanth, V. (2023, November). Combining Neural Networks to Recognize Offline Digits & Words by Training the Model Using Keras. In 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE) (pp. 694-697). IEEE.
21. Jain, R. (2018). Beyond stateless: A production architecture for running distributed databases on Kubernetes at scale. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 1(2), 416–423.
22. Padmanabham, S. (2025). AI-Augmented Business Process Automation: Architecture and Implementation in Regulated Industries. Journal Of Multidisciplinary, 5(7), 983-991.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805038

23. Badam, L. R. (2022). Machine learning-based catastrophic loss prediction for climate-related insurance risk. International Journal of Future Innovative Science and Technology (IJFIST), 5(1), 7797–7807.
24. Patel, K., Pilgar, C., & Thakare, S. B. (March 2025). Agile Hardware Development: A Cross-Industry Exploration for Faster Prototyping and Reduced Time-to-Market. In 4th World Conference on Mechanical Engineering (pp. 1–15). Indian Institute of Information Technology Design and Manufacturing Kancheepuram.
25. Anand, L. (2023). Distributed Multi-Cloud Data Lake and Edge Computing Architecture for Intelligent SAP Enterprise Data Integration. International Journal of Computer Technology and Electronics Communication, 6(5), 7636-7344.
26. Mathew, A. (2023). Sentinel AI: An Investigation into Robust Threat Mitigation Strategies for Artificial Intelligence. Educational Research (IJMCER), 5(5), 108-111.
27. Polamarasetty, V. K. (2023). Modern enterprise HR technology through Workday-based benefits and absence management. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(4), 6908–6913.
28. Patel, C. (2024). AI-driven recommendation systems for improving online customer journey. International Journal of Current Engineering and Technology, 14(6), 549–556. https://doi.org/10.14741/ijcet/v.14.6.18
29. Ravichandran, S., & Kandasamy, V. (2025). Optimized Attention Augmented Residual Convolutional Neural Network with Fa-Resnet for Fabric Defect Detection. Journal of Control Engineering and Applied Informatics, 27(4), 3-15.
30. Pothuri, M. K. Building a Seamless Healthcare Data Fabric: Zero-Touch Integration and Scalable Mapping Across Provider, Claims, Recipient, and Pharmacy Source Systems for State Medicaid. IJLRP-International Journal of Leading Research Publication, 6(8).
31. Ahuja, D. (2025). DevOps and Ethical AI: Ensuring Responsible Deployment. Journal Of Multidisciplinary, 5(6), 1-14.
32. Matrouk, K., V, S., Kumar, S., Bhadla, M. K., Sabirov, M., & Saadh, M. J. (2023). Deep Learning–based Dynamic User Alignment in Social Networks. ACM Journal of Data and Information Quality, 15(3), 1-26.
33. Vemireddy, S. (2024). Secure and scalable intelligent service architectures for next-generation enterprise applications. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8177–8182.
34. Kundavaram, R. R., Bandhela, R. R., & Onteddu, A. R. (2022). AI-driven predictive modeling in healthcare: A data science perspective on U.S. healthcare data. South Eastern European Journal of Public Health. https://doi.org/10.70135/seejph.vi.6691
35. Selvarajan, K. (2022). Architecting scalable self-service data platforms for enterprise analytics. International Journal of Science, Research and Technology (IJSRAT), 5(2), 7427–7436.
36. Bitragunta, S. L. V. (2024). A novel AI-blockchain-edge framework for fast and secure transient stability assessment in smart grids. International Journal For Multidisciplinary Research, 6(6).
37. Tanha, T. T., Anonna, S. A., & Basnet, Y. (2025). Machine Learning Framework for Liver Cirrhosis Stage Prediction Using Clinical and Biochemical Features. Frontiers in Computer Science and Artificial Intelligence, 4(1), 84-97.
38. Patel, K. (2024). Human–machine collaboration in microbiological laboratories: A posthuman perspective on automation, control, and scientific agency. Journal of Posthumanism, 4(3), 2346–2355. https://doi.org/10.63332/joph.v4i3.4186
39. Nisar, K. (2024). Prompting, retrieval, and fine-tuning: Foundations of enterprise language model adaptation. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(6), 9310-9319.
40. Chundi, V. R. K. (2025). AI-based Sustainable Vehicle Monitoring System for Existing Internal Combustion Vehicles. London Journal of Research In Computer Science and Technology, 25(3), 1-7.
41. Venkatasalam, K., Rajendran, P., & Thangavel, M. (2019). Improving the accuracy of feature selection in big data mining using accelerated flower pollination (AFP) algorithm. Journal of medical systems, 43(4), 96.
42. Pothuri, M. K. Building a Seamless Healthcare Data Fabric: Zero-Touch Integration and Scalable Mapping Across Provider, Claims, Recipient, and Pharmacy Source Systems for State Medicaid. IJLRP-International Journal of Leading Research Publication, 6(8).
43. Himeluzzaman, M., Alam, A., Gazi, M. S., Abdullah, S. M., Chy, M. S. K., Onik, T. A., Nabil, M. A., & Shakil, S. M. (2025). Countering AI-generated disinformation: A novel detection model to safeguard national security. International Journal of Computer Technology and Electronics Communication, 8(4), 11192–11203.